PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-126425
(43)Date of publication of application : 11.05.1999

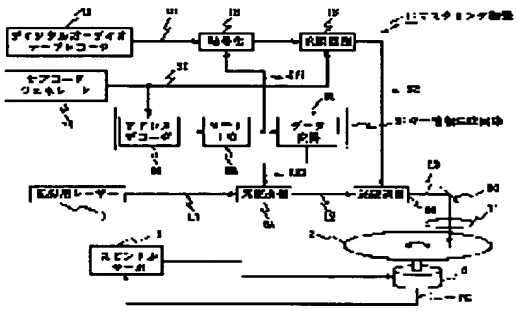
(51)Int.Cl. G11B 20/10
G11B 7/00

(21)Application number : 09-292071
(22)Date of filing : 24.10.1997

(71)Applicant : SONY CORP
(72)Inventor : KOBAYASHI SEIJI

(54) OPTICAL DISK DEVICE, OPTICAL DISK REPRODUCING METHOD AND OPTICAL DISK

(57)Abstract:
PROBLEM TO BE SOLVED: To make the analysis of encipherment difficult by obtaining a procedure, which is necessary for detecting from an optical disk a key information required for the release of encipherment, from outside an equipment other than the optical disk, and thereby changing the cryptographic method.
SOLUTION: A digital signal processor, after generating a seek command to a servo circuit in response to a user's operation, binarizes with a prescribed threshold value the envelope detection result of a digital reproducing signal DRF obtained from the seek, and reproduces key information KY2. In addition, through a process corresponding to a data conversion circuit 9C at the time of recording, the key information KY2 is parallelly converted to form key information KY1, releasing the encipherment of a digital audio signal reproduced from a compact disk, in accordance with the processing program of a floppy disk supplied with the compact disk in pairs. Then, by the change of various processing procedures, the detection procedure of the key information KY2 is made changeable, as is data processing procedure or the like.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－126425

(43)公開日　平成11年(1999)５月11日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
7/00		7/00	Ｒ

審査請求　未請求　請求項の数13　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－292071

(22)出願日　平成９年(1997)10月24日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　小林　誠司
東京都品川区北品川６丁目７番35号　ソニー株式会社内

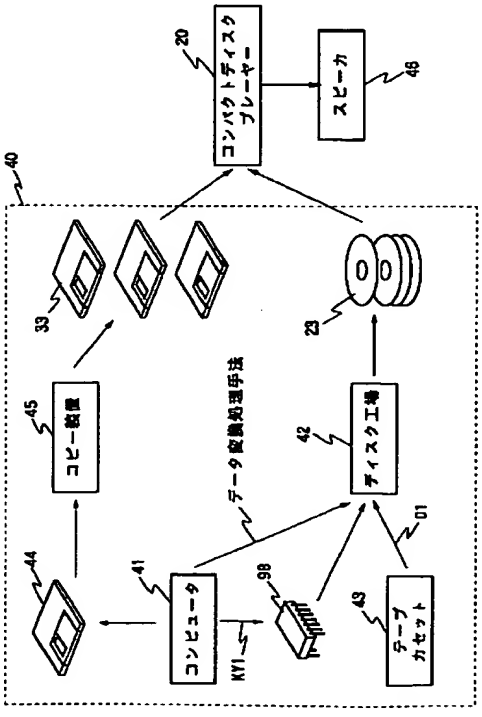
(74)代理人　弁理士　多田　繁範

(54)【発明の名称】　光ディスク装置、光ディスクの再生方法及び光ディスク

(57)【要約】

【課題】本発明は、光ディスク装置、光ディスクの再生方法及び光ディスクに関し、例えばコンパクトディスクと、その再生装置及び再生方法に適用して、従来に比して一段と確実に違法コピーを防止できるようにする。

【解決手段】暗号化の解除に必要なキー情報を光ディスク２３より検出するのに必要な手順を、光ディスク２３以外の機器の外部３３より取得する。



【特許請求の範囲】
【請求項１】光ディスクにレーザービームを照射して前記光ディスクを再生する光ディスク装置において、
前記レーザービームの戻り光に応じて信号レベルが変化する再生信号を生成する再生信号生成手段と、
前記再生信号を２値識別して第１のディジタル信号を再生する第１の再生信号処理手段と、
所定のキー情報を用いて前記第１のディジタル信号の暗号を解除する暗号処理手段と、
前記光ディスクより、前記キー情報の生成に必要な第２のディジタル信号を検出する信号検出手段と、
所定の処理手順により、前記第２のディジタル信号より前記キー情報を生成するキー情報生成手段と、
前記処理手順を、前記光ディスク以外の機器の外部より取得して前記キー情報生成手段に設定する入力手段とを備えることを特徴とする光ディスク装置。
【請求項２】前記光ディスクは、
ピット又はマークの幅により前記第２のディジタル信号が記録され、
前記信号検出手段は、
前記再生信号の信号レベルを検出して信号レベル検出結果を出力する信号レベル検出手段と、
前記信号レベル検出結果に基づいて、前記第２のディジタル信号を再生する識別手段とを有することを特徴とする請求項１に記載の光ディスク装置。
【請求項３】前記入力手段は、
前記光ディスクとは異なる所定の記録媒体より前記処理手順を取得することを特徴とする請求項１に記載の光ディスク装置。
【請求項４】前記入力手段は、
所定の伝送路を介して前記処理手順を取得することを特徴とする請求項１に記載の光ディスク装置。
【請求項５】光ディスクにレーザービームを照射して前記光ディスクを再生する光ディスク装置において、
前記レーザービームの戻り光に応じて信号レベルが変化する再生信号を生成する再生信号生成手段と、
前記再生信号を２値識別して第１のディジタル信号を再生する第１の再生信号処理手段と、
所定のキー情報を用いて前記第１のディジタル信号の暗号を解除する暗号処理手段と、
前記光ディスクより、前記キー情報の生成に必要な第２のディジタル信号を検出する信号検出手段と、
所定の処理手順により、前記第２のディジタル信号より前記キー情報を生成するキー情報生成手段とを備え、
前記キー情報生成手段は、
前記処理手順が前記光ディスク以外により変更可能に設定されたことを特徴とする光ディスク装置。
【請求項６】光ディスクにレーザービームを照射して前記光ディスクを再生する光ディスク装置において、
前記レーザービームの戻り光に応じて信号レベルが変化する再生信号を生成する再生信号生成手段と、
前記再生信号を２値識別して第１のディジタル信号を再生する第１の再生信号処理手段と、
所定のキー情報を用いて前記第１のディジタル信号の暗号を解除する暗号処理手段と、
所定の検出手順により、前記光ディスクより、前記キー情報の生成に必要な第２のディジタル信号を検出する信号検出手段と、
前記第２のディジタル信号より前記キー情報を生成するキー情報生成手段と、
前記検出手順を、前記光ディスク以外の機器の外部より取得して前記信号検出手段に設定する入力手段とを備えることを特徴とする光ディスク装置。
【請求項７】前記光ディスクは、
ピット又はマークの幅により前記第２のディジタル信号が記録され、
前記信号検出手段は、
前記検出手順により指定される箇所より、前記再生信号の信号レベルを検出して信号レベル検出結果を出力する信号レベル検出手段と、
前記信号レベル検出結果に基づいて、前記第２のディジタル信号を再生する識別手段とを有することを特徴とする請求項６に記載の光ディスク装置。
【請求項８】前記入力手段は、
前記光ディスクとは異なる所定の記録媒体より前記検出手順を取得することを特徴とする請求項６に記載の光ディスク装置。
【請求項９】前記入力手段は、
所定の伝送路を介して前記検出手順を取得することを特徴とする請求項６に記載の光ディスク装置。
【請求項１０】光ディスクにレーザービームを照射して前記光ディスクを再生する光ディスク装置において、
前記レーザービームの戻り光に応じて信号レベルが変化する再生信号を生成する再生信号生成手段と、
前記再生信号を２値識別して第１のディジタル信号を再生する第１の再生信号処理手段と、
所定のキー情報を用いて前記第１のディジタル信号の暗号を解除する暗号処理手段と、
所定の検出手順により、前記光ディスクより、前記キー情報の生成に必要な第２のディジタル信号を検出する信号検出手段と、
前記第２のディジタル信号より前記キー情報を生成するキー情報生成手段とを備え、
前記信号検出手段は、
前記検出手順が前記光ディスク以外により変更可能に設定されたことを特徴とする光ディスク装置。
【請求項１１】光ディスクにレーザービームを照射して得られる戻り光を２値識別して第１のディジタル信号を再生し、
所定の処理手順により、前記光ディスクより検出した第

２のディジタル信号よりキー情報を生成し、
前記キー情報により前記第１のディジタル信号の暗号化を解除する光ディスクの再生方法であって、
前記処理手順を、前記光ディスク以外の機器の外部より取得することを特徴とする光ディスクの再生方法。
【請求項１２】光ディスクにレーザービームを照射して得られる戻り光を２値識別して第１のディジタル信号を再生し、
所定の検出手順により前記光ディスクより第２のディジタル信号を検出し、
前記第２のディジタル信号よりキー情報を生成し、
前記キー情報により前記第１のディジタル信号の暗号を解除する光ディスクの再生方法であって、
前記検出手順を、前記光ディスク以外の機器の外部より取得することを特徴とする光ディスクの再生方法。
【請求項１３】所定のキー情報により暗号化された第１のディジタル信号と、所定の処理手順により前記キー情報に変換される第２のディジタル信号とが記録され、
前記処理手順が所定の情報伝達手段により伝達されることを特徴とする光ディスク。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、光ディスク装置、光ディスクの再生方法及び光ディスクに関し、例えばコンパクトディスクと、その再生装置及び再生方法に適用することができる。本発明は、暗号化の解除に必要なキー情報を光ディスクより検出するのに必要な手順を、光ディスク以外の機器の外部より取得することにより、従来に比して一段と確実に違法コピーを防止できるようにする。
【０００２】
【従来の技術】従来、コンパクトディスクにおいては、リードインエリアの内周側に、製造メーカー、製造場所、ディスク番号等を示す符号が刻印され、この符号を目視確認することにより他のコンパクトディスクと識別できるようになされている。
【０００３】
【発明が解決しようとする課題】ところでこの刻印によって記録されるメーカー等の符号は、目視によって認識することを目的とするものである。このため違法コピーを完全には防止できない問題がある。
【０００４】このような問題を解決する１つの方法として、ピット幅の変化により識別データを発見困難に記録する方法が考えられる。ところがこのような方法でも、違法コピーの業者に一旦違法コピーの識別方法が判明すると、模倣させる恐れがあり、完全に違法コピーを防止できない問題がある。
【０００５】本発明は以上の点を考慮してなされたもので、従来に比して一段と確実に違法コピーを防止することができる光ディスク装置、光ディスクの再生方法及び光ディスクを提案しようとするものである。
【０００６】
【課題を解決するための手段】かかる課題を解決するため本発明においては、光ディスク装置及び光ディスクの再生方法に適用して、光ディスクより検出した第２のディジタル信号よりキー情報を生成する処理手順を、光ディスク以外の機器の外部より取得してキー情報生成手段に設定する。
【０００７】また光ディスク装置に適用して、光ディスクより検出した第２のディジタル信号よりキー情報を生成する処理手順を、光ディスク以外により変更可能にする。
【０００８】また光ディスク装置及び光ディスクの再生方法に適用して、キー情報の生成に必要な第２のディジタル信号を光ディスクより検出する検出手順を、光ディスク以外の機器の外部より取得して信号検出手段に設定する。
【０００９】また光ディスク装置に適用して、キー情報の生成に必要な第２のディジタル信号を光ディスクより検出する検出処理手順を、光ディスク以外により変更可能に設定する。
【００１０】また光ディスクに適用して、所定のキー情報により暗号化された第１のディジタル信号と、所定の処理手順によりこのキー情報に変換される第２のディジタル信号とを記録し、先の処理手順が所定の情報伝達手段により伝達されるようにする。
【００１１】第２のディジタル信号より所定の処理手順でキー情報を生成し、このキー情報より第１のディジタル信号の暗号化を解除する場合、第２のディジタル信号及び処理手順とが正しい対応関係にあるときだけ、第１のディジタル信号の暗号化を正しく解除することができる。このような関係を前提にして、この処理手順を光ディスク以外の機器の外部より取得してキー情報生成手段に設定すれば、必要に応じてこの処理手順を変更することができる。これにより例えば定期的に、第１のディジタル信号の暗号化、第２のディジタル信号を変更し、この変更に対応するように処理手順を変更して、処理手順、光ディスクを解析して実行される違法コピーを防止することができる。
【００１２】またこの処理手順を光ディスク以外により変更可能に設定して、同様に、違法コピーに対応することができる。
【００１３】またキー情報の生成に必要な第２のディジタル信号を光ディスクより検出する検出手順を、光ディスク以外の機器の外部より取得して信号検出手段に設定しても、例えば定期的に、第１のディジタル信号の暗号化、第２のディジタル信号を変更し、この変更に対応するように検出手順を変更して、検出手順、光ディスクを解析して実行される違法コピーを防止することができる。

【００１４】またキー情報の生成に必要な第２のディジタル信号を光ディスクより検出する検出手順を、変更可能に設定すれば、同様に、違法コピーに対応することができる。

【００１５】また光ディスクに適用して、所定のキー情報により暗号化された第１のディジタル信号と、所定の処理手順によりこのキー情報に変換される第２のディジタル信号とを記録するようにし、この処理手順が所定の情報伝達手段により伝達されるようにすれば、同様にして、違法コピーに対応することができる。

【００１６】

【発明の実施の形態】以下、適宜図面を参照しながら本発明の実施の形態を詳述する。

【００１７】図２は、マスタリング装置を示すブロック図である。この実施の形態においては、必要に応じてこのマスタリング装置が選択され、このマスタリング装置１よりディスク原盤２を順次露光し、コンパクトディスクのマザーディスクを作成する。

【００１８】すなわちこのマスタリング装置１において、スピンドルモータ４は、スピンドルサーボ回路５の制御によりディスク原盤２を所定の回転速度で回転駆動する。このときスピンドルモータ４は、底部に取付けられた周波数発電機により、ディスク原盤２が所定角度だけ回転する毎に信号レベルが切り換わるＦＧ信号ＦＧを出力する。

【００１９】スピンドルサーボ回路５は、このＦＧ信号ＦＧを基準にして、スピンドルモータ４の回転速度を制御し、いわゆる線速度一定（ＣＬＶ：Constant Linear Velocity）の条件によりスピンドルモータ４の回転を制御する。

【００２０】記録用レーザー７は、例えばガスレーザーにより構成され、レーザービームＬ１を光変調器８Ａに射出する。光変調器８Ａ及び光変調器８Ｂは、例えば電気音響光学素子により構成される。このうち光変調器８Ａは、キー情報生成回路９から供給されるキー情報ＫＹ２に従ってレーザービームＬ１の光量を変化させる。すなわちキー情報ＫＹ２の論理レベルが論理１の場合、レーザービームＬ１を減衰させることなく射出し、キー情報ＫＹ２の論理レベルが論理０の場合、レーザービームＬ１を所定光量だけ減衰させて射出する。

【００２１】光変調器８Ｂは、光変調器８Ａより射出されるレーザービームＬ２をＥＦＭ（Eight to Fourteen Modulation）信号Ｓ２に応じてオン／オフ制御して射出する。

【００２２】ミラー１０は、光変調器８Ｂより射出されるレーザービームＬ３の光路を折り曲げて、ディスク原盤２に向けて射出する。対物レンズ１１は、このミラー１０の反射光をディスク原盤２の記録面上に集光する。これらミラー１０及び対物レンズ１１は、図示しないスレッド機構により、ディスク原盤２の回転に同期して半径方向に順次移動するようになされ、これによりマスタリング装置１では、ディスク原盤２の内周側から外周側に向かって、ラセン状にトラックを形成し、このトラック上にＥＦＭ信号Ｓ２に対応したピット形状を形成する。

【００２３】さらにこのときレーザービームＬ１の光量を光変調器８Ａにより制御することにより、キー情報ＫＹ２に応じてピット幅が変化するようにディスク原盤２を露光し、これによりピット幅の変化によりキー情報ＫＹ２を記録する。

【００２４】ディジタルオーディオテープレコーダ１２は、このディスク原盤２に記録するディジタルオーディオ信号Ｄ１を出力する。サブコードジェネレータ１３は、このディジタルオーディオ信号Ｄ１のタイムコード（時、分、秒、フレームにより構成される）を生成する。さらにサブコードジェネレータ１３は、このタイムコードより、ディスク原盤２に記録するサブコードデータＳＣを生成して出力する。なおサブコードジェネレータ１３は、リードインエリアに記録するＴＯＣのデータも併せて生成し、対応するタイミングにより出力する。

【００２５】キー情報生成回路９は、このサブコードデータＳＣのタイムコードより、キー情報ＫＹ１及びＫＹ２を生成する。すなわちキー情報生成回路９は、アドレスデコーダ９Ａにサブコードデータ ＳＣを入力し、ここでタイムコードをデコードする。メモリＩＣ９Ｂは、ビット情報を保持するリードオンリメモリ又はＥＰ－ＲＯＭで構成され、タイムコードをアドレスにしてＤＥＳ（Data Encryption Standard）符号による５４ビットのキー情報ＫＹ１を出力する。これによりキー情報生成回路９は、ディジタルオーディオ信号Ｄ１の処理単位でなるフレーム毎に、タイムコードに対応するキー情報ＫＹ１を出力する。

【００２６】データ変換回路９Ｃは、この５４ビットのキー情報ＫＹ１を第２のキー情報ＫＹ２に変換して出力する。ここでこのデータ変換回路９Ｃは、このマスタリング装置１により作成するコンパクトディスクの仕様に応じてデータ変換処理の内容が設定され、例えばキー情報ＫＹ１をシリアルデータに変換することにより、また仕様に応じて、配列を変更し、変調することにより、第２のキー情報ＫＹ２を生成する。なおこの実施の形態では、データ変換回路９Ｃは、キー情報ＫＹ１を単にシリアルデータに変換して出力する。

【００２７】暗号化回路１５は、第１のキー情報ＫＹ１により、ディジタルオーディオ信号Ｄ１を暗号化して出力する。

【００２８】変調回路１６は、暗号化回路１５より出力されるオーディオデータをコンパクトディスクについて規定されたフォーマットに従ってデータ処理することにより、ＥＦＭ信号Ｓ２を生成する。すなわち変調回路１６は、オーディオデータをフレーム単位で区切り、サブ

コードジェネレータ１３から供給されるサブコードデータＳＣを順次割り当ててフレーム構造を形成する。さらに各フレームに誤り訂正符号を付加した後、インターリーブ処理し、さらにＥＦＭ変調することによってＥＦＭ信号Ｓ２を生成する。

【００２９】この実施の形態に係るコンパクトディスクの製造工程は、このディスク原盤２を現像した後、さらに電鋳処理することによってマザーディスクを作成し、このマザーディスクを用いてスタンパーを作成する。さらにこのスタンパーを用いた射出成形により、ディスク状基板を形成し、このディスク状基板に反射膜、保護膜を順次作成してコンパクトディスクを作成する。

【００３０】これによりこのマスタリング装置１を用いて作成されたコンパクトディスクは、暗号化されたディジタルオーディオ信号Ｄ１がピット列の繰り返しにより記録され、この暗号化のキー情報ＫＹ１から所定の処理手順により生成されたキー情報ＫＹ２がピット幅の変化により記録されるようになされている。

【００３１】図３は、このようにして作成されたコンパクトディスクを再生するコンパクトディスクプレイヤーを示すブロック図である。このコンパクトディスクプレイヤー２０において、スピンドルモータ２１は、サーボ回路２２の制御によりコンパクトディスク２３を線速度一定の条件により回転駆動する。

【００３２】光ピックアップ２４は、コンパクトディスク２３にレーザービームを照射して得られる戻り光より、この戻り光の光量に応じて信号レベルが変化する再生信号ＲＦを生成する。さらに光ピックアップ２４は、サーボ回路２２の制御により、コンパクトディスク２３の半径方向に可動し、これにより所望のトラックをシークできるようになされている。

【００３３】２値化回路２５は、この再生信号ＲＦを２値化して２値化信号を生成した後、この２値化信号より再生クロックを生成する。さらに２値化回路２５は、この再生クロックを基準にして２値化信号を順次ラッチすることにより、再生信号ＲＦから再生データＢＤを再生する。

【００３４】ＥＦＭ復調回路２６は、この再生データＢＤをＥＦＭ復調して出力する。ＥＣＣ回路２７は、ＥＦＭ復調回路２６の出力データをデインターリーブ処理した後、この出力データに付加された誤り訂正符号により誤り訂正処理して出力する。

【００３５】暗号処理回路２８は、ＥＣＣ回路２７の出力データを受け、ディジタル信号処理プロセッサー（ＤＳＰ）３０より出力されるキー情報ＫＹ１により暗号化を解除して出力する。

【００３６】ディジタルアナログ変換回路（Ｄ／Ａ）２９は、この暗号処理回路２８の出力データをディジタルアナログ変換処理し、これによりアナログ信号によるオーディオ信号ＳＡを出力する。

【００３７】このようなオーディオデータの再生系に対して、アナログディジタル変換回路（Ａ／Ｄ）３１は、再生クロックＣＫを基準にして再生信号ＲＦをアナログディジタル変換処理し、これによりディジタル再生信号ＤＲＦを生成して出力する。

【００３８】ディジタル信号処理プロセッサー３０は、図４に示す処理手順を実行することにより、コンパクトディスク２３の再生開始時、フロッピーディスク３３により供給される処理手順をロードする。さらにディジタル信号処理プロセッサー３０は、この処理手順に従ってキー情報ＫＹ１を生成し、このキー情報ＫＹ１を暗号処理回路２８にセットする。

【００３９】ここでこの処理手順は、ピット幅の変化により記録された第２のキー情報ＫＹ２を検出する検出手順と、この第２のキー情報ＫＹ２よりキー情報ＫＹ１を生成するデータ処理手順とにより構成される。

【００４０】この検出手順において、ディジタル信号処理プロセッサー３０は、ディジタル再生信号ＤＲＦより、再生信号ＲＦの信号レベルを検出してピット幅の変化を検出する。さらにフロッピーディスク３３により供給される処理手順に従って、サーボ回路２２を制御して、コンパクトディスク２３の所望のトラックよりピット幅の変化を検出できるようになされている。

【００４１】またデータ処理手順において、ディジタル信号処理プロセッサー３０は、ピット幅の変化により検出されるディジタル信号を、マスタリング装置１のデータ変換回路９Ｃに対応した処理により処理できるようになされている。

【００４２】ディジタル信号処理プロセッサー３０は、図４に示す処理手順において、ステップＳＰ１からステップＳＰ２に移り、フロッピーディスク３３より処理手順でなるプログラムをロードする。続いてディジタル信号処理プロセッサー３０は、ステップＳＰ３に移り、この処理手順に含まれる検出手順に従ってコンパクトディスク２３よりキー情報ＫＹ２を取得し、さらにこの処理手順に含まれるデータ処理手順によりキー情報ＫＹ２からキー情報ＫＹ１を生成する。ディジタル信号処理プロセッサー３０は、続くステップＳＰ４において、このキー情報ＫＹ１を暗号処理回路２８にセットした後、ステップＳＰ５に移ってこの処理手順を終了する。

【００４３】この実施の形態においては、ディジタル信号処理プロセッサー３０は、ロードしたプログラムにより、この一連の処理のうちのステップＳＰ３及びステップＳＰ４の処理手順を、コンパクトディスク２３より得られる再生データのフレーム単位で実行し、これにより記録時に対応した処理によりキー情報ＫＹ１を生成する。

【００４４】すなわちディジタル信号処理プロセッサー３０は、ユーザーの操作に応動してサーボ回路２２にシークコマンドを発行した後、シークより得られるディジ

タル再生信号ＤＲＦをエンベロープ検波する。さらにこのエンベロープ検波結果を所定のしきい値により２値化し、これによりキー情報ＫＹ２を再生する。記録時のデータ変換回路９Ｃに対応する処理により、さらにこのキー情報ＫＹ２をパラレル変換処理し、これによりキー情報ＫＹ１を生成する。

【００４５】これによりこのコンパクトディスクプレイヤー２０では、コンパクトディスク２３と対により供給されるフロッピーディスク３３の処理プログラムに従ってコンパクトディスク２３より再生されるディジタルオーディオ信号の暗号化を解除するようになされ、フロッピーディスク３３より供給される処理手順の変更により種々の処理手順によりキー情報ＫＹ２の検出手順、キー情報ＫＹ２からキー情報ＫＹ１を生成するデータ処理手順を変更できるようになされている。

【００４６】図１は、マスタリング装置１及びコンパクトディスクプレイヤー２０の関係を示す模式図である。コンパクトディスクの製造側４０では、コンパクトディスクプレイヤー２０で再生可能であるとの条件を満たす範囲で、キー情報ＫＹ２の記録位置、如何なるタイムコードとの関係等によりキー情報ＫＹ１を生成するかが決定され、これによりコンパクトディスク２３の仕様が決定される。

【００４７】コンピュータ４１は、オペレータの操作により、この決定した仕様により、図２について上述したメモリＩＣ９Ｂに記録するキー情報ＫＹ１を生成する。コンパクトディスクの製造側４０では、このキー情報ＫＹ１をメモリＩＣ９Ｂに記録してディスク工場４２に供給する。またデータ変換回路９Ｃのデータ変換処理を記録した情報を、ディジタルオーディオ信号を記録したテープカセット４３と共に、ディスク工場４２に供給する。

【００４８】ディスク工場４２は、コンパクトディスクの仕様に応じて、マスタリング装置１を選択する。さらにメモリＩＣ９Ｂをマスタリング装置１にセットし、またデータ変換回路９Ｃのデータ変換処理をセットし、この条件によりテープカセット４３に記録されたディジタルオーディオ信号をディスク原盤２に記録する。さらにこのディスク原盤２よりコンパクトディスク２３を作成する。

【００４９】またコンピュータ４１は、コンパクトディスクプレイヤーにおいて、キー情報ＫＹ２を検出する検出手順、この再生したキー情報ＫＹ２よりキー情報ＫＹ１を作成するデータ処理手順による処理プログラムをフロッピーディスク４４に記録する。

【００５０】コンパクトディスクの製造側４０では、コピー装置４５において、このフロッピーディスク４４の内容がコピーされて、図３について上述したフロッピーディスク３３が作成され、コンパクトディスク２３とフロッピーディスク３３との組み合わせがユーザーに供給される。

【００５１】以上の構成において、コンパクトディスクの製造側４０では（図１）、コンパクトディスク２３の仕様が決定されると、この決定に従ってコンピュータ４１によりディジタルオーディオ信号を暗号化するキー情報ＫＹ１が作成され、このキー情報ＫＹ１がメモリＩＣ９Ｂに記録されてディスク工場４２に供給される。またコンパクトディスク２３に記録するキー情報ＫＹ２をキー情報ＫＹ１より生成するデータ変換手法が、ディスク工場４２に連絡される。

【００５２】これに対応してディスク工場４２では、このコンパクトディスクの作成にマスタリング装置１が選択され（図２）、さらにマスタリング装置１のキー情報生成回路９にメモリＩＣ９Ｂがセットされ、データ変換回路９Ｃのデータ変換処理が連絡されたデータ変換手法にセットされる。

【００５３】これによりマスタリング装置１では、ディジタルオーディオ信号Ｄ１の各フレームのタイムコードによりメモリＩＣ９Ｂがアクセスされ、このメモリＩＣ９Ｂに格納されたキー情報ＫＹ１によりディジタルオーディオ信号Ｄ１が暗号化される。さらにこのディジタルオーディオ信号Ｄ１にサブコードデータＳＣ、誤り訂正符号が付加され、ＥＦＭ変調されてＥＦＭ信号Ｓ２が生成される。マスタリング装置１では、回転するディスク原盤２にレーザービームＬ３を照射し、このレーザービームＬ３がＥＦＭ信号Ｓ２によりオンオフ制御されることにより、ＥＦＭ信号Ｓ２に応じたピット形状が順次ディスク原盤２に露光される。

【００５４】この処理と平行して、マスタリング装置１では、データ変換回路９Ｃにおいて、コンピュータ４１により通知されたデータ変換処理によりキー情報ＫＹ１がキー情報ＫＹ２にデータ変換処理され、このキー情報ＫＹ２に応じてレーザービームＬ１の光量が切り換えられる。コンパクトディスクの製造工場では（図１）、このようにして露光されたディスク原盤２よりコンパクトディスク２３が作成され、これによりピット幅の変化によりキー情報ＫＹ２が記録される。

【００５５】このようにしてピット幅が変化するように作成されたコンパクトディスク２３においては、保護膜、反射膜を剥離してディスク状基板よりスタンパーを作成するコピー方法においては、ピット幅の変化が損なわれ、これにより違法コピーの作成が困難化される。またコンパクトディスクを再生して得られるＥＦＭ信号等によりコピーのコンパクトディスクを作成する場合、ピット幅の変化が失われることにより、この種の方法による違法コピーが防止される。

【００５６】このようにしてコンパクトディスク２３を作成する他方で、コンパクトディスクの製造側４０では、コンパクトディスク２３に記録したキー情報ＫＹ２を検出する検出手順、キー情報ＫＹ２よりキー情報ＫＹ

１を作成するデータ処理手順がフロッピーディスク３３に記録され、このフロッピーディスク３３がコピーされ、コンパクトディスク２３と組み合わされて、ユーザーに提供される。

【００５７】これにより正規の流通ルートにより流通する正規のコンパクトディスクについては、対応するフロッピーディスク３３が組み合わされることにより、コンパクトディスクより得られるディジタルオーディオ信号を正しく暗号解除することができる。これに対してこのコンパクトディスクの暗号化を解析して作成される違法コピーのコンパクトディスクに対しては、定期的に、キー情報ＫＹ２の記録位置、キー情報ＫＹ１からキー情報ＫＹ２を生成するデータ変換手法、キー情報ＫＹ１自体等を変更することにより、実質的に解析困難にすることができる。またこれらの関係でなる暗号化の手法が解析されて違法コピーが作成されたとしても、これらの関係等を変更することにより、フロッピーディスク３３により提供される処理手順との対応関係を誤ったものとすることができ、これにより暗号化されたディジタルオーディオ信号の正しい再生を困難にすることができる。

【００５８】すなわちユーザー側においては（図３）、この組み合わされて提供されたコンパクトディスク２３及びフロッピーディスク３３がコンパクトディスクプレイヤー２０にセットされ、再生開始時、フロッピーディスク３３に記録された処理手順がディジタル信号処理プロセッサー３０にロードされる。コンパクトディスクプレイヤー２０では、このロードされた処理手順の検出手順に従って、再生信号ＲＦがアナログディジタル変換回路３１によりディジタル再生信号ＤＲＦに変換され、このディジタル再生信号ＤＲＦのエンベロープがディジタル信号処理プロセッサー３０で検出されてキー情報ＫＹ２が検出される。

【００５９】さらにロードされた処理手順に含まれるデータ処理手順に従って、このキー情報ＫＹ２がパラレルデータでなるキー情報ＫＹ１に変換され、このキー情報ＫＹ１が順次暗号処理回路２８にセットされる。これによりコンパクトディスクプレイヤー２０においては、暗号処理回路２８において、コンパクトディスク２３を再生して得られるデータ列の暗号化が解除され、その結果得られるディジタルオーディオ信号がアナログ信号に変換されて出力される。

【００６０】以上の構成によれば、暗号化して記録されたディジタルオーディオ信号を再生する際に、フロッピーディスク３３より提供される検出手順に従って、ピット幅により記録されたキー情報ＫＹ２を検出し、同様にして提供されるデータ処理手順に従ってこのキー情報ＫＹ２をキー情報ＫＹ１に変換して暗号化を解除することにより、またこの検出手順、データ処理手順を光ディスク以外の外部機器でなるフロッピーディスク３３により変更可能に設定したことにより、必要に応じて暗号化の手順を変更して、これに対応するように検出手順、データ処理手順を変更することができる。これにより必要に応じて暗号化を変更して暗号処理の解析による違法コピーの作成を困難にすることができ、また違法コピーされた場合でも正しい再生を困難にすることができ、これらにより従来に比して一段と確実に違法コピーを防止することができる。

【００６１】またピット幅により記録した第２のキー情報ＫＹ２を検出することにより、違法にコピーされたコンパクトディスクについては、このピット幅により記録されたキー情報ＫＹ２を複製困難にすることができ、これによっても違法コピーを排除することができる。

【００６２】なお上述の実施に形態においては、順次変化するサブコードデータに対応して順次キー情報ＫＹ１を切り換える場合について述べたが、本発明はこれに限らず、特定のキー情報ＫＹ１により暗号化する場合にも広く適用することができる。なおこの場合、図２について上述したマスタリング装置１においては、メモリＩＣ９Ｂより固定値のキー情報ＫＹ１を出力することにより対応することができる。またキー情報ＫＹ２については、コンパクトディスク２３の特定アドレスについてだけ記録することができ、この場合に他の箇所にはダミーの情報、さらにはキー情報ＫＹ１、ＫＹ２の検出、データ変換に参考とする一部情報等を記録することもできる。またコンパクトディスクプレイヤー２０においては、再生開始時、フロッピーディスク３３より供給される処理手順に従って、この特定アドレスを再生してキー情報ＫＹ２を検出することにより対応することができる。なおこれらは、上述の実施に形態に対して、ピット幅により記録した第２のディジタル信号の検出手順を変更する関係にある。

【００６３】また上述の実施に形態においては、キー情報ＫＹ１を単にパラレルデータに変換してキー情報ＫＹ２を記録する場合について述べたが、本発明はこれに限らず、パラレルデータに変換した後、配列を変更して記録する場合、種々の変調方式により変調して記録する場合等、種々のデータ変換方式を広く適用することができる。なおこの場合、図２について上述したマスタリング装置１においては、データ変換回路９Ｃのデータ変換処理を変更することにより対応することができる。またコンパクトディスクプレイヤー２０においては、フロッピーディスク３３より供給されるデータ処理手順に従って、検出したキー情報ＫＹ２をデータ処理することにより対応することができる。なおこれらは、上述の実施に形態に対して、第２のディジタル信号よりキー情報を生成するデータ処理手順を変更する関係にある。

【００６４】さらに上述の実施の形態においては、ピット幅の変化によりキー情報ＫＹ２でなる第２のディジタル信号を記録する場合について述べたが、本発明はこれに限らず、例えば故意にピット誤りを形成して第２のデ

ィジタル信号を記録する場合、ピット長の変位により第２のディジタル信号を記録する場合等にも広く適用することができる。この場合、コンパクトディスクプレイヤーにおいて、これらの何れの方式にも対応できるようにし、フロッピーディスク３３より提供される検出手順に従ってこれら何れかの方式により記録された第２のディジタル信号、又はこれらの組み合わせにより記録された第２のディジタル信号を検出することになる。

【００６５】また上述の実施の形態においては、コンパクトディスク以外の外部の機器としてフロッピーディスクにより処理手順を提供する場合について述べたが、本発明はこれに限らず、例えばフラッシュメモリなどのメモリチップにより処理手順を提供してもよく、さらには電話回線等の通信回線により提供してもよい。

【００６６】さらに上述の実施の形態においては、本発明をコンパクトディスクに適用する場合について述べたが、本発明はこれに限らず、ＤＶＤ等、種々の光ディスク及び光ディスク再生装置に広く適用することができる。

【００６７】

【発明の効果】上述のように本発明によれば、暗号化の解除に必要なキー情報を光ディスクより検出するのに必要な手順を、光ディスク以外の機器の外部より取得することにより、必要に応じて暗号化手法を変更して、暗号化の解析を困難にすることができ、また暗号化の解析により違法コピーが作成された場合でも、正しい再生を困難にすることができる。これにより従来に比して一段と確実に違法コピーを防止することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るコンパクトディスクの製造工程等を示す模式図である。

【図２】図１の工程に適用されるマスタリング装置を示すブロック図である。

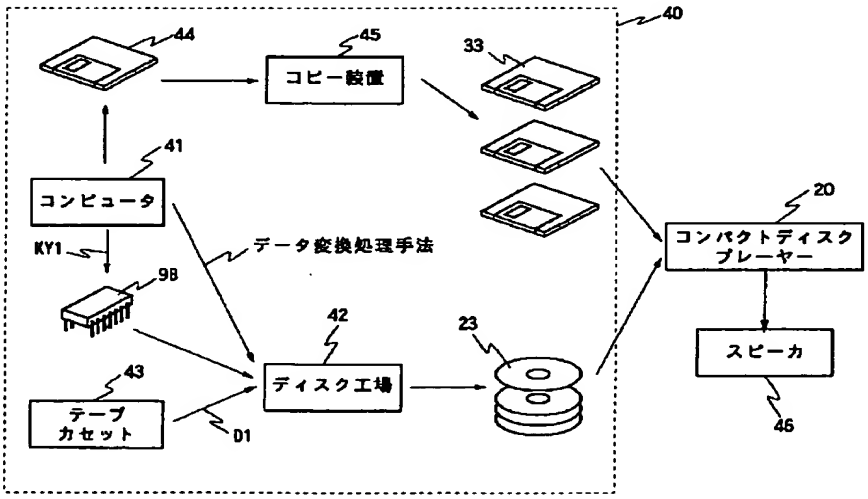
【図３】図２のマスタリング装置により作成されたコンパクトディスクの再生に使用されるコンパクトディスクプレイヤーを示すブロック図である。

【図４】図３のコンパクトディスクプレイヤーにおけるディジタル信号処理プロセッサーの処理手順を示すフローチャートである。

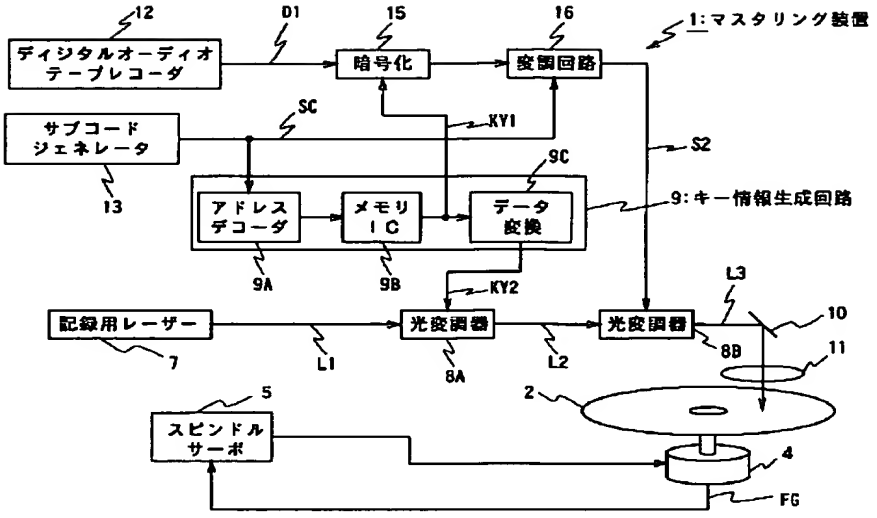
【符号の説明】

１……マスタリング装置、２……ディスク原盤、９……キー情報生成回路、９Ａ……アドレスデコーダ、９Ｂ……メモリＩＣ、９Ｃ……データ変換回路、２０……コンパクトディスクプレイヤー、２３……コンパクトディスク、３１……アナログディジタル変換回路、３０……ディジタル信号処理プロセッサー、３３、４４……フロッピーディスク

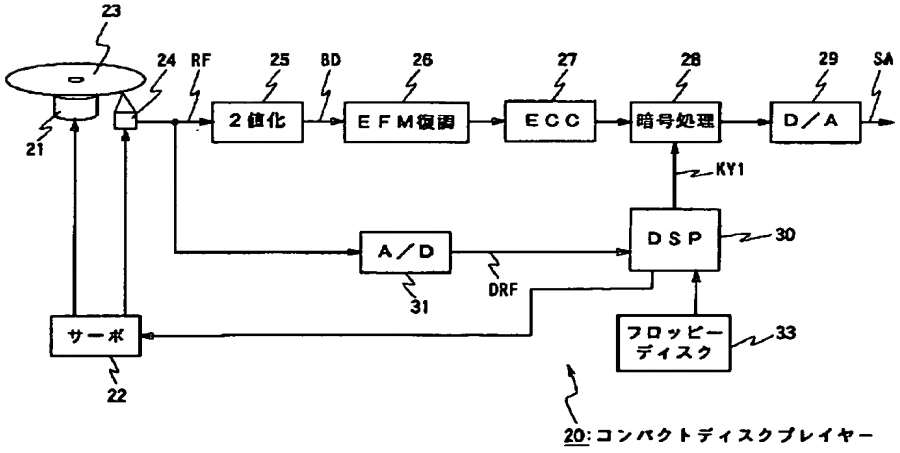
【図１】



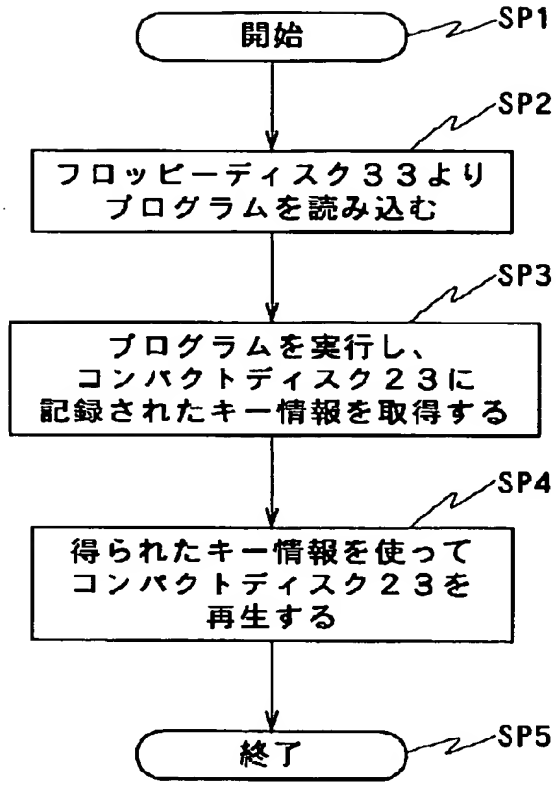
【図２】


12
D1
15
16
1:マスタリング装置
ディジタルオーディオテープレコーダ
暗号化
変調回路
SC
KY1
S2
サブコードジェネレータ
13
9C
アドレスデコーダ
メモリIC
データ変換
9:キー情報生成回路
9A
9B
KY2
L3
10
記録用レーザー
光変調器
光変調器
8B
11
7
L1
8A
L2
5
2
スピンドルサーボ
4
FG

【図３】


23
24
RF
25
8D
26
27
28
29
SA
2値化
EFM復調
ECC
暗号処理
D/A
21
KY1
A/D
DSP
30
31
DRF
サーボ
フロッピーディスク
33
22
20:コンパクトディスクプレイヤー

【図４】


開始
SP1
SP2
フロッピーディスク３３より
プログラムを読み込む
SP3
プログラムを実行し、
コンパクトディスク２３に
記録されたキー情報を取得する
SP4
得られたキー情報を使って
コンパクトディスク２３を
再生する
終了
SP5

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-187013
(43)Date of publication of application : 09.07.1999

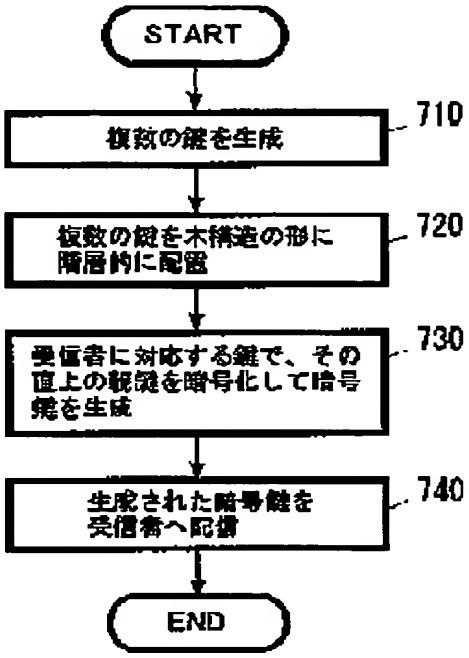
(51)Int.Cl. H04L 9/08
G09C 1/00

(21)Application number : 09-354401
(22)Date of filing : 24.12.1997

(71)Applicant : IBM JAPAN LTD
(72)Inventor : MARUYAMA HIROSHI
TOKUYAMA TAKESHI
URAMOTO NAOHIKO

(54) CRYPTOGRAPHIC KEY DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a system for minimizing procedures required for updating a cryptographic key by structuring the cryptographic key into tree structure.
SOLUTION: First of all, plural keys more than the number of recipients are generated 710, and the plural keys are hierarchically arranged 720 in the form of tree structure. Next, the plural recipients are made correspondent to the keys hierarchically arranged in the form of tree structure, and the cryptographic keys of the respective recipients are generated as a key stream having keys from the root of tree structure to positions corresponding to the said recipients in the tree structure. Thus, after the cryptographic key is generated 730, the generated cryptographic key is distributed 740 to the correspondent recipient.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]